サイバースパイとサイバー攻撃——スパイ機関創設批判の論点整理

2026年3月27日(金)19時

としまる

toshi@jca.apc.org

本日のセミナーの概要

- イランに対する米国・イスラエルの侵略戦争の場合を例に米国防総省 (戦争省) の発表

  先制攻撃に先立つサイバースパイとサイバー先制攻撃

  必須条件としての官民連携：米軍 + 民間 (AWS+Parantir+Anthropics)
- これまでの戦争との違いとは
- サイバー領域をめぐる反戦運動の新しい課題

※ 今回は、サイバー領域におけるいわゆる「情報戦」や SNS の役割については扱いません。これらは次回に扱います。

※ 今回は、主に米国 (米軍) の動向を中心に扱います。イスラエルの動向は扱っていません。

イランに対する米国・イスラエルの侵略戦争の場合

3/2 国防総省記者会見 ダン・ケイン統合参謀本部議長 (制服組のトップ)

- この作戦 (「エピック・フューリー作戦」（壮絶な怒り）など) に直接関与：中央軍（ CENTCOM ）
- 作戦への支援：米宇宙軍（ USSPACECOM ）、米サイバー軍（ USSCYBERCOM ）、米欧州軍（ USEUCOM ）
- 空爆に先立つ攻撃：米サイバー軍（ USCYBERCOM ）と米宇宙軍（ USSPACECOM ）⇒ イランの視認・通信・対応能力を妨害・弱体化・遮断

  ※空爆だけが先制攻撃なのではなく、空爆に先行したサイバー攻撃が不可欠な行動であった。
- 2 月 28 日 主要戦闘作戦の開始：米国情報機関の支援により、イスラエル国防軍が直接攻撃。陸上、海上、戦闘機、給油機、空中早期警戒・電子攻撃機、爆撃機、そして無人機など、 100 機以上の航空機が米国本土から一斉に離陸。
- 中央軍（ CENTCOM ）は、イラン側の指揮統制インフラ、海軍部隊、弾道ミサイル基地、および情報インフラを体系的に標的とし、敵を混乱させ、動揺させることに重点を置く。
- 宇宙・サイバー作戦の連携により、責任区域全域の通信網やセンサーネットワークを効果的に遮断し、敵が状況を把握し、連携し、効果的に対応する能力を喪失。
- 最高指導者ハメネイなど主要な権力者たちを殺害。その後も殺害が続く。民間の犠牲者も多数。

イランに対する米国・イスラエルの侵略戦争の場合

イランの視認・通信・対応能力を妨害・弱体化・遮断

主要戦闘作戦の開始

中央軍
CENTCOM

物理的標的
指揮統制インフラ
海軍部隊
弾道ミサイル基地

標的の殺害、破壊

物理的標的
情報インフラ

通信網やセンサーネットワークを遮断

状況把握、連携・効果的対応能力を奪う

米サイバー軍
USCYBERCOM

米宇宙軍
USSPACECOM

注：この図式は米国防総省の発表によるものなのでイスラエルの役割は反映されていない

※数日でイラン国内で１２５０カ所以上の標的を攻撃し、イラン艦船１１隻を破壊 (ロイター)

イランに対する米国・イスラエルの侵略戦争の場合

3/2 国防総省記者会見 ダン・ケイン将軍

この作戦に直接関与している他の戦闘指揮部、すなわち米宇宙軍（USSPACECOM）、米サイバー軍（USSCYBERCOM）、および米欧州軍（USEUCOM）による、中央軍（CENTCOM）の作戦への支援について、特に強調しておきたい。

先陣を切ったのは米サイバー軍（USCYBERCOM）と米宇宙軍（USSPACECOM）であり、非物理的効果を重ねて、イランの視認・通信・対応能力を妨害・弱体化・遮断しました。主要戦闘作戦の開始時刻である H-Hour 、現地東部夏時間午前 1 時 15 分（テヘラン時間午前 9 時 45 分）、中央軍管区全域に夜明けが差し込む中、空は一気に活気づきました。陸上、海上、戦闘機、給油機、空中早期警戒・電子攻撃機、爆撃機、そして無人機など、 100 機以上の航空機が米国本土から一斉に離陸し、単一の同期した波を形成しました。これは、米国情報機関の支援により、イスラエル国防軍が引き金を引くこととなった昼間の攻撃でした。

作戦開始から約 57 時間が経過しました。初期段階において、中央軍（CENTCOM）は、イラン側の指揮統制インフラ、海軍部隊、弾道ミサイル基地、および情報インフラを体系的に標的とし、敵を混乱させ、動揺させることに重点を置きました。宇宙・サイバー作戦の連携により、責任区域全域の通信網やセンサーネットワークを効果的に遮断し、敵が状況を把握し、連携し、効果的に対応する能力を喪失させました。

https://www.war.gov/News/Transcripts/Transcript/Article/4418959/secretary-of-war-pete-hegseth-and-chairman-of-the-joint-chiefs-of-staff-gen-dan/

イランに対する米国・イスラエルの侵略戦争の場合

3/2 国防総省記者会見 ヘグセス国防長官

「いわゆる国際機関が何を言おうと、アメリカは史上最も破壊力が高く、かつ精密な空爆作戦を展開している。 B-2 爆撃機、戦闘機、無人機、ミサイル、そしてもちろん機密扱いの兵器も投入されている。すべては我々の条件に基づき、最大限の権限を行使して行われている。**愚かな交戦規則も、国家再建という泥沼も、民主主義構築の試みも、政治的に正しい戦争などない。**我々は勝利のために戦い、時間や人命を無駄にすることはない。」

「力による平和」、戦士の精神、戦闘能力、目的の一致――これらは単なるスローガンではない。それらは、軍服、あの軍服を身にまとうことの意味そのものの、鼓動する心臓なのだ。砲火の下でも冷静に判断し、混乱の中でも果断に行動し、躊躇なく憲法を守り、祖国を守る。**我々はもはや「防衛者」ではない。我々は戦士だ。敵を殺し、その意志を砕くために鍛え上げられた戦士である。**歴史が見ている。誓いを立てた通りの存在となれ。集中し、規律を守り、命を惜しまず、決して折れない存在となれ。」

「我々は、トランプ大統領が定めた「アメリカ第一」の条件の下でこれを成し遂げる。」

「全能の神があなたを見守り、その摂理の御手によってあなたを包み込んでくださいますように。戦士たちよ、神の御加護を。そして、前へ進み続けなさい。」

※ヘグセスは、これまでも既存の国内法、国際法よりも軍が戦争で勝利する上で必要な能力を上位に置くことを繰り返し主張してきた。

https://www.war.gov/News/Transcripts/Transcript/Article/4418959/secretary-of-war-pete-hegseth-and-chairman-of-the-joint-chiefs-of-staff-gen-dan/

イランに対する米国・イスラエルの侵略戦争の場合：サイバースパイ

テヘランの交通カメラのほぼすべて
<u>長年にわたりハッキング</u>

日常的な車の駐車
場所を特定

イスラエルに
暗号化されて
情報を送信

携帯電話ネットワーク
のハッキング

人間による
情報提供

プロファイルに追加

護衛、運転手の
個人情報のプロファイル

<u>**住所、勤務時間、通勤ルート、誰の担当なのかなど「生活パターン」を把握**</u>

アルゴリズム主導による膨大なデータ収集と作業の自動化

出典： https://www.ft.com/content/bf998c69-ab46-4fa3-aae4-8f18f7387836

イランに対する米国・イスラエルの侵略戦争の場合：サイバースパイ

様々な情報や報道からわかること

Financial Times

「イラン高官の精鋭で忠実な護衛や運転手が、テヘランのパスツール通り付近（土曜日にイスラエルの空爆でアヤトラ・アリ・ハメネイが殺害された場所）で勤務に就いた際、イスラエル側は彼らを監視していた。

この件に詳しい２人の関係者によると、**テヘランの交通カメラのほぼすべてが<u>長年にわたりハッキング</u>**されており、その映像は暗号化されてテルアビブとイスラエル南部のサーバーに送信されていたという。

あるカメラの画角が特に有用だったと、関係者の一人は述べた。これにより、彼らは男たちが自家用車をどこに駐車するのが好きかを特定でき、厳重に警備された施設内のありふれた<u>**日常の営みを覗き見る手がかり**</u>を手にしたのだ。

複雑なアルゴリズムにより、<u>**警備員たちの個人ファイルに詳細が追加された。そこには住所、勤務時間、通勤ルート、そして最も重要な点として、彼らが通常誰の護衛や送迎を担当しているか**</u>が含まれており、情報将校たちが「生活パターン」と呼ぶものを構築していた。」

https://www.ft.com/content/bf998c69-ab46-4fa3-aae4-8f18f7387836?syn-25a6b1a6=1

イランに対する米国・イスラエルの侵略戦争の場合

様々な情報や報道からわかること

Financial Times

「個々の標的を追跡することは、かつては視覚的な確認や誤情報の選別を必要とする骨の折れる作業だったが、**イスラエルのアルゴリズム主導による膨大なデータ収集により、近年その作業は自動化されていた。**

しかし、ハメネイのような極めて重要な標的の場合、失敗は許されなかった。イスラエルの軍事教義では、互いに独立して活動する２人の上級将校が、標的が攻撃対象の場所に確実にいること、そして誰と共に行動しているかを高い確度で確認することが要件となっている。

この件に詳しい２人の関係者によると、**イスラエル情報機関は、ハッキングされた交通カメラや携帯電話ネットワーク深くへの侵入など、信号情報からの情報を得ていた。**そのうちの１人は、ハメネイとの会合が予定通り行われ、高官たちがその場所へ向かっていることが示されていたと述べた。

しかし、状況に詳しい両者によると、アメリカ側にはさらに具体的な情報源――**人間による情報提供者**がいたという。CIA はコメントを控えた。」

https://www.ft.com/content/bf998c69-ab46-4fa3-aae4-8f18f7387836?syn-25a6b1a6=1

イランに対する米国・イスラエルの侵略戦争の場合

様々な情報や報道からわかること

Financial Times

イラン側はどのようなサイバー行動をとっていたか

「2022 年、イランの治安機関と関係のあるグループが、モサド長官の妻の携帯電話から盗み出したとされるデータを公開した。また、**2025 年の戦争中、イランはエルサレムの監視カメラをハッキングし、イスラエル側が放送で検閲したリアルタイムの被害状況を把握**した。さらに、ミサイル防衛システムの写真を購入し、イスラエル検事によれば、イスラエル市民に賄賂を贈って**主要政治家のジョギングルートを地図化**までしていたという。」

https://www.ft.com/content/bf998c69-ab46-4fa3-aae4-8f18f7387836?syn-25a6b1a6=1

イランに対する米国・イスラエルの侵略戦争の場合

様々な情報や報道からわかること

BBC

「戦争のこの段階では、戦闘員がオープンソース情報、衛星画像分析、サイバースパイ活動を活用してイラン国内の軍事目標を特定するため、サイバー戦が重要な役割を果たす可能性が高い。

この作業においても、**人工知能（AI）ツールが積極的に活用**されている可能性が高い。その兆候は、ヘグセス長官が実戦中の情報工作員を称賛した発言からもう一度窺える。」

https://www.bbc.com/news/articles/c5yr0576ygvo

イランに対する米国・イスラエルの侵略戦争の場合

ハメネイ殺害の経緯——事前監視

- ネットワークへのハッキング (侵入)
- 地域全体を監視対象に
- 数年の長期間にわたって監視
- 標的だけでなく、関係者を幅広く監視
- 人びとの日常生活の習慣を把握
- そもそも標的が最初から決められているとは限らず、作戦の経緯に応じて標的がどのように変更されても対応できるよな網羅的な情報を収集
- 街頭の監視カメラ、ネット遮断など相手国のネットワークがもっている自国の市民を監視する仕組みを逆用

イランに対する米国・イスラエルの侵略戦争の場合

現在進行中のイランの戦争からの教訓

- 実空間（キネティック）の攻撃とサイバー攻撃は不可分一体
- 実空間の先制攻撃に先立つサイバー先制攻撃
- 年単位の長期にわたるサイバースパイ行為による膨大なデータ収集
- サイバースパイは相手国の監視カメラや通信ネットワークを転用

※今回は「情報戦」に関する問題を扱っていませんが、SNS での情報操作や偽情報、大衆運動の扇動など、従来の戦争プロパガンダにはない重要な課題があります。この件については次回に取り上げます。

イランに対する米国・イスラエルの侵略戦争の場合

Anthropic の AI 「Claude」、 Palantir、 Amazon Web Services と国防総省など政府組織との連携があったと報じられている。ただし、イラン戦争での具体的な役割は明かではない。

- 街頭監視カメラ網のハッキング
- インターネットの遮断
- 携帯電話基地局をハッキングして通話機能を妨害

- 反政府運動の扇動
- 宗教暦アプリ「BadeSaba」の乗っ取り
- 国営放送などの妨害

数年にわたるサイバースパイ活動

- サイバースパイ活動は数年にわたる
- 実空間の攻撃に先行する「先鋒」の役割を担う
- 民間企業のインフラとノウハウが不可欠
- サイバースパイ、サイバー攻撃の全体像は不明なままになる場合が多い

官民連携について

米国防総省は、 2026 年 2 月 28 日に実施された米国とイスラエルによるイラン施設への共同**空爆の初期段階において、軍事目標の特定と優先順位付けを行うため、 Anthropic 社が開発した人工知能モデル「 Claude 」と、 Palantir Technologies 社が構築した「 Maven Smart System 」を併用した。**

この空爆は、イスラム革命防衛隊（ IRGC ）の基地、ミサイル貯蔵庫、指揮センター、その他の軍事インフラを含む、 **2,000 カ所以上のイラン施設を標的とした米国とイスラエルの共同作戦の一環**として実施された。作戦開始から最初の 24 時間の間に、**統合された「 Claude-Maven 」システムは約 1,000 の優先順位付けされた標的を生成**し、それぞれに軍事計画担当者が使用する詳細な作戦データが付随していた。

初期攻撃における AI 支援による標的特定

同プログラムに詳しい国防当局者によると、 Claude は複数の情報の流れを同時に処理した。これには衛星画像、信号情報、監視データ、偵察フィードが含まれる。このモデルはこれらの入力を分析し、**それぞれの攻撃候補に対して正確な GPS 座標、推奨される兵器システム、および自動的に生成された法的根拠を含む標的リストを作成**した。

出力結果は **Palantir 社の Maven Smart System を通じて提供された。同システムは、米軍司令部が作戦計画や情報分析に使用する中核的な分析プラットフォームとして機能**している。この統合により、指揮官は従来の情報ワークフローで**通常必要とされる数日や数週間ではなく、数時間以内に標的パッケージを作成できる**ようになった。

この作戦は、米中央軍を含む米軍の指揮系統の下で実施された。同軍は、 5 万人以上の米軍兵士、約 200 機の戦闘機、 2 隻の空母が参加した地域キャンペーンを統括し、空爆を指揮した。

(thedefensenews.com) 米国防総省、イラン空爆で 1,000 の標的を特定するために Anthropic の AI 「 Claude 」と Palantir の「 Maven 」を使用 https://www.thedefensenews.com/news-details/Pentagon-Used-Anthropics-Claude-AI-and-Palantir-Maven-to-Identify-1000-Targets-in-Iran-Strikes/

官民連携について

2024年11月に以下のような報道があり、かなり話題になった。

「Anthropic社とPalantir Technologies社は、Amazon Web Services（AWS）との提携を発表し、米国の情報機関および防衛機関に対し、AWS上で「Claude 3」および「Claude 3.5」モデルファミリーへのアクセスを提供することになった。この提携により、AWSが提供するセキュリティ、俊敏性、柔軟性、および持続可能性のメリットを活かしながら、PalantirのAI Platform（AIP）内でClaudeを活用するための統合技術スイートが実現する。」

https://www.businesswire.com/news/home/20241107699415/en/Anthropic-and-Palantir-Partner-to-Bring-Claude-AI-Models-to-AWS-for-U.S.-Government-Intelligence-and-Defense-Operations

官民連携について

Anthropic、Palantir Technologies、Amazon Web Services（AWS）はいずれも日本でも活動している企業。AnthropicのAI、Claudeは私たちでも利用できる。Parantirは民間や自治体などだけでなく有力な軍事関連のサービスも展開している。



https://www.palantir.com/jp/solutions/public/defense/



https://www.anthropic.com/



https://aws.amazon.com/

上のサイトの記事は「AWS 活用で実現する同盟国間の防衛機密情報と技術共有」

https://aws.amazon.com/jp/blogs/news/allies-can-share-data-and-technologies-and-remain-compliant-with-international-regulations-using-aws/

官民連携について

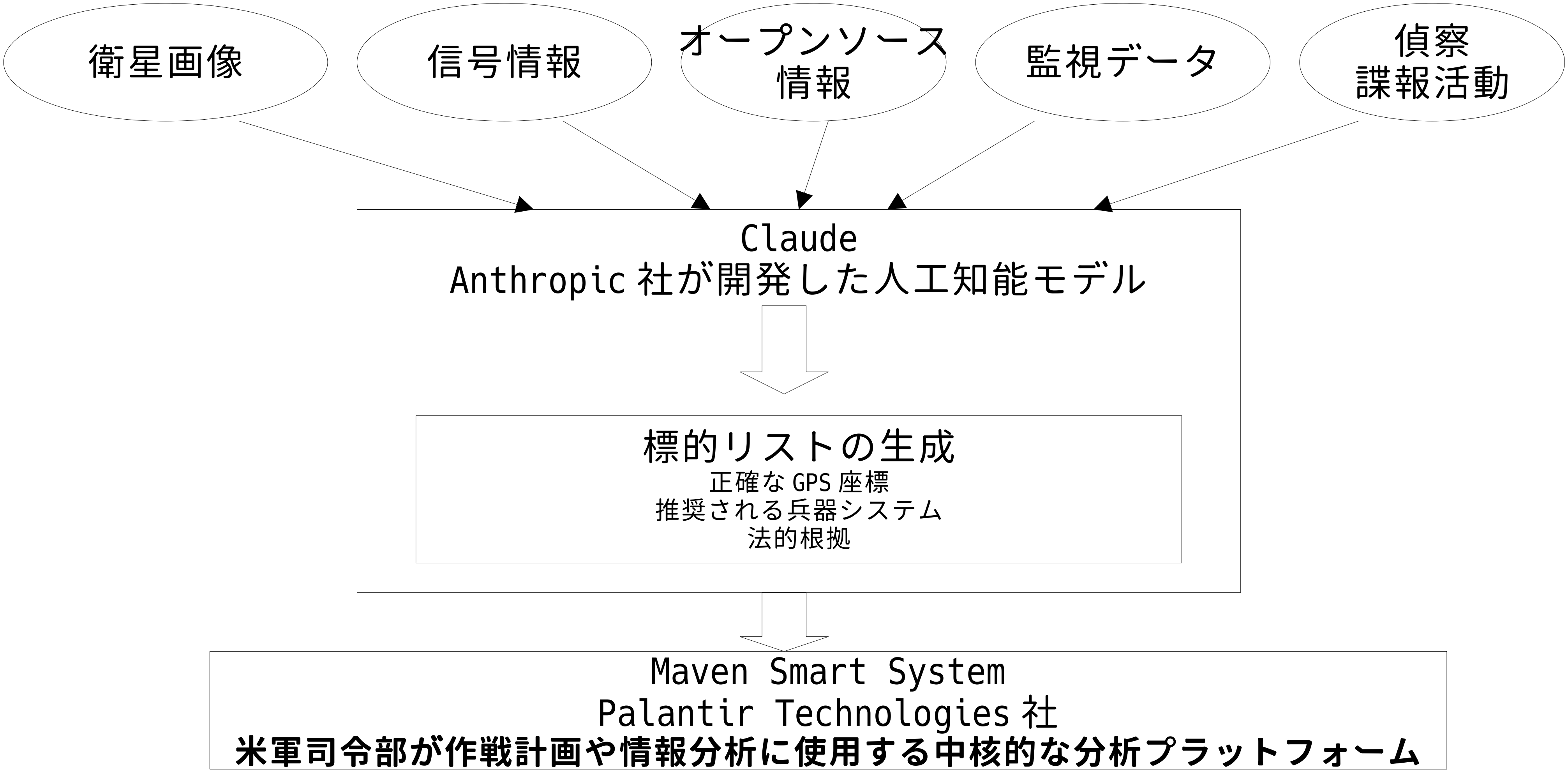
6　パランティア・テクノロジーズへの訪問

1月16日、小泉防衛大臣は、ワシントンD.C.にあるAIおよびデータ分析プラットフォームを開発する企業、パラントア・テクノロジーズを訪問した。同大臣は同社の事業について説明を受け、地域の安全保障情勢について協議した。



小泉防衛大臣 2026 年 1 月訪米で Parantir を訪問
防衛省 https://www.mod.go.jp/en/article/2026/01/3eee3a5675cfbb9312ca9962baf1f5dc7547e1da.html

イラン戦争での官民連携について



https://www.thedefensenews.com/news-details/Pentagon-Used-Anthropics-Claude-AI-and-Palantir-Maven-to-Identify-1000-Targets-in-Iran-Strikes/

イラン戦争での官民連携について

- ドローンの映像分析に機械学習を適用するために2017年に米国防総省が立ち上げたAlgorithmic Warfare Cross-Functional Team（アルゴリズム戦争横断機能チーム）と呼ばれものの後継のシステム。
- 2024年末、AnthropicのAI「Claude」は、PalantirとAmazon Web Servicesの提携を通じてMavenに統合された。この統合により、AIモデルが機密扱いの軍事環境内で稼働できるようになる。

  Mavenとは「画像やフルモーションビデオなどの戦場データを処理し、状況認識を向上させ、意思決定を迅速化」するシステム。同システムを運用する兵士を8時間の実習コースで訓練できる。

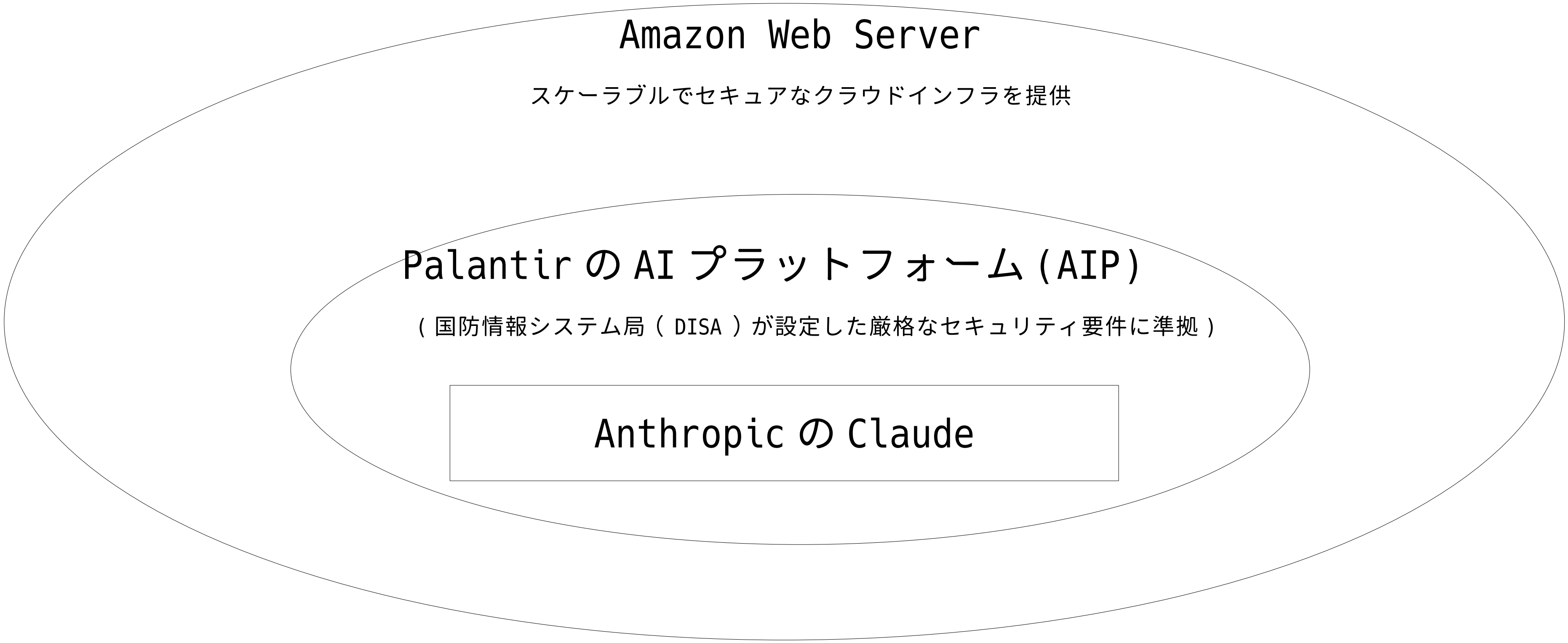
  米陸軍 https://www.army.mil/article/290958/armys_combined_arms_command_to_integrate_maven_c2_smart_system_into_training_and_education
- 2025年6月、Anthropicは「Claude Gov」と呼ばれる政府向けバージョンを導入。これは国家安全保障機関による利用を特に想定して設計されたもの。
- Claudeは、機密扱いの防衛ネットワークに組み込まれた最初の大規模生成AIシステムの一つとなり、情報分析、作戦計画支援、戦場シナリオの自動シミュレーションなどの機能を提供した。

出典 defencenews.com

https://www.thedefensenews.com/news-details/Pentagon-Used-Anthropics-Claude-AI-and-Palantir-Maven-to-Identify-1000-Targets-in-Iran-Strikes/

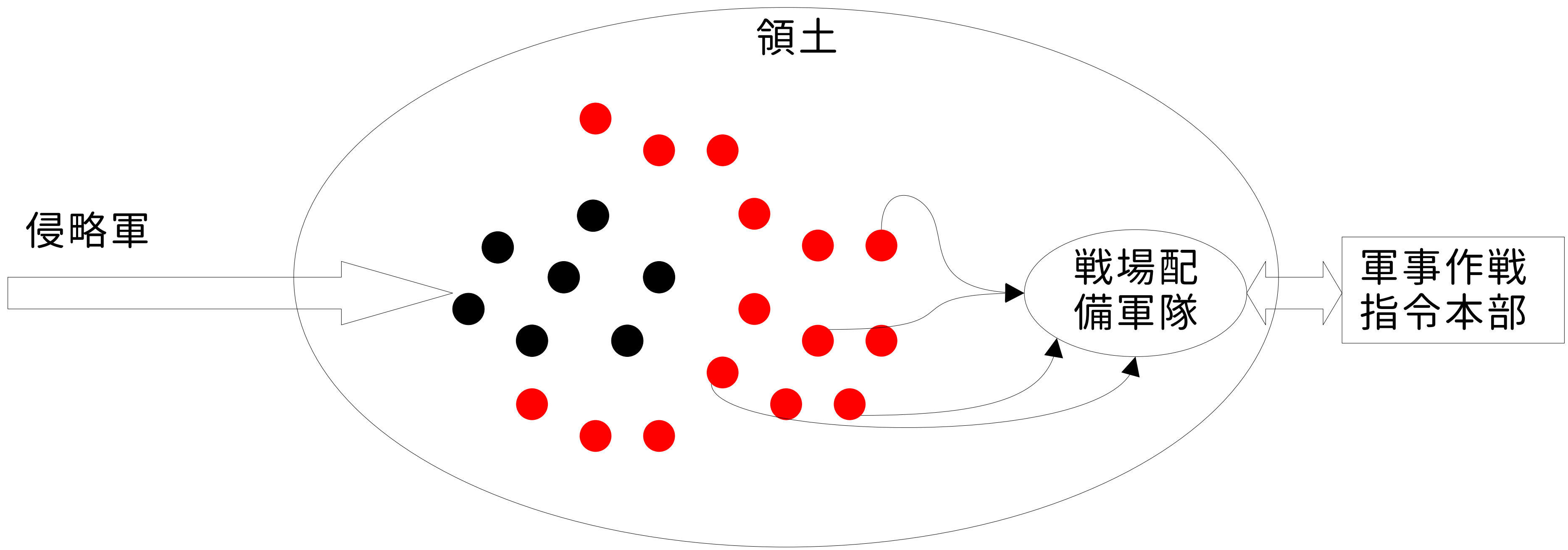
イランに対する米国・イスラエルの侵略戦争の場合

2024 年末、 Anthropic の AI 「 Claude 」は、 Palantir と Amazon Web Services の提携を通じて Maven に統合された。この統合により、 AI モデルが機密扱いの軍事環境内で稼働できるようになる。



Palantir と AWS は、最も厳格なセキュリティプロトコルを要件とする国防情報システム局（ DISA ）の IL6 認定を取得

これまでの戦争

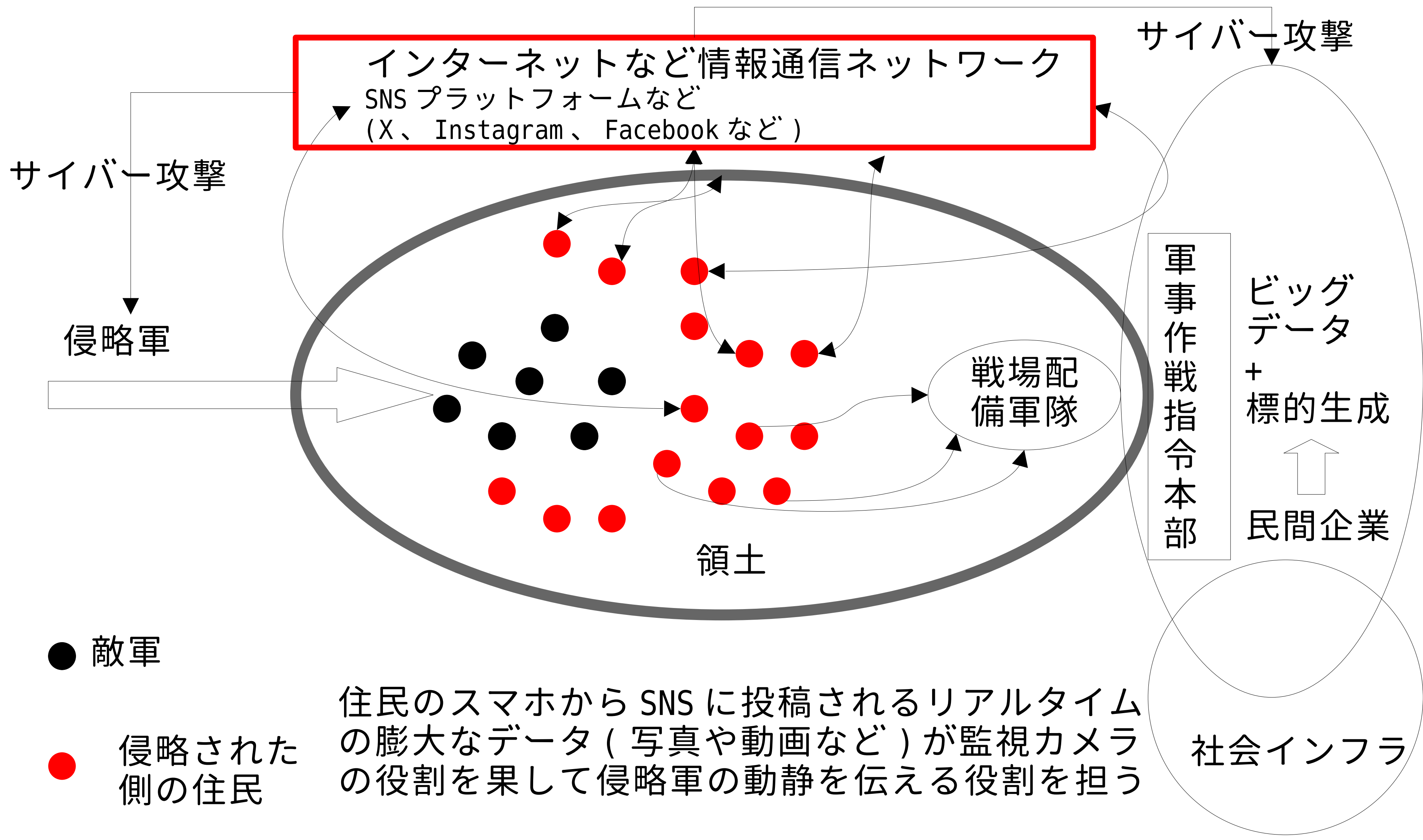


● 敵軍

● 侵略された側の住民

•戦場になっている地域の住民からの限られた情報
•偵察等によって得られた情報
これらを基に反撃の戦術を練ることになる。

SNS などネットの発信が社会インフラになっている場合



住民のスマホから SNS に投稿されるリアルタイムの膨大なデータ (写真や動画など) が監視カメラの役割を果して侵略軍の動静を伝える役割を担う

サイバー領域をめぐる反戦運動の新しい課題

- サイバースパイ 長期にわたる秘密の活動
  - 網羅的な情報収集
  - 相手国政府の監視システムを転用
  - 違法なハッキングなどサイバー攻撃のを性格をもつ
  - 情報操作など「サイバー戦」の手段でもある
- 自国政府の監視システムや住民データは、同時に相手国にとっての格好の監視・情報収集の標的になる。

サイバー領域をめぐる反戦運動の新しい課題

- サイバー攻撃は従来の武力行使と複雑に絡み合う
  - サイバー攻撃なき実空間の武力攻撃はありえない
  - サイバー攻撃は先制攻撃の手段でもある
  - サイバースパイとサイバー攻撃は不可分である
- 官民連携でなければサイバースパイ・サイバー攻撃は実施できない。
  - 莫大な情報通信インフラは外資を含む民間が保有
  - 最先端のサイバー軍事技術は民間が先行
  - 民間の軍事技術はわたしたちのネット関連サービスとも密接に関連し、軍事と民生の境界があいまい

サイバー領域をめぐる反戦運動の新しい課題

法や制度への反対運動は、従来からの反戦・平和運動でも行なわれてきた。しかし、サイバー領域の戦争にはそれ以上の取り組みが必要になる。

- サイバー領域の戦争は法制度によって効果的に阻止できるとは限らない。法の支配を過信できない領域でもある。(コンピュータに人権も法律も理解できない)⇒ 法だけでなく、技術がもたらす戦争への加担を阻止することが必須。
- 膨大な個人データが戦争における重要な資源に なる。⇒個人情報を可能な限り政府、民間企業問わず第三者に渡さない工夫
- 情報戦に加担しないこと。対抗的な情報発信が必要になる。ネットは情報を受けるためだけでなく、政府や戦争を煽る言論への対抗の場でもある。(次回のテーマ)
- 民生用技術の軍事転用が容易になっている。戦争に加担する企業のサービスを使わない。
- 国境を越えた連帯をつくりだす。インターネットは国境を越えた民衆のインフラでもある。「敵国」の民衆とともに、それぞれの国や企業の戦争への加担を阻止すること、ネットの検閲や遮断を回避すること、抑圧や弾圧にあっている人たちへの支援などのネットワークを構築するなど、多くのことがネットを介した連帯運動として可能。